COUNCIL OF THE EUROPEAN UNION

Brussels, 24 August 2006

Interinstitutional File: 2005/0202 (CNS)

11547/2/06 REV 2

LIMITE

CRIMORG 124
DROIPEN 44
ENFOPOL 146
DATAPROTECT 26
COMIX 642

NOTE

From :	Presidency
To :	Multidisciplinary Group on Organised Crime
No. prev. doc. :	6450/5/06 REV 5 CRIMORG 31 DROIPEN 13 ENFOPOL 29 DATAPROTECT 5 COMIX 174
Subject :	Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

1. On 4 October 2005, the Commission forwarded a Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters to the Secretary-General of the Council. On 13 December 2005, the Council asked the Parliament for its opinion on the proposal.
The European Data Protection Supervisor has delivered his opinion on the proposal[1], which he presented to the MDG-Mixed Committee on 12 January 2006. On 24 January 2006, the Conference of European Data Protection Authorities also delivered an opinion on the proposal[2]. On 11 January 2006, the Hungarian delegation submitted an extensive note on the Commission proposal[3].

[1] doc. 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864.
[2] doc. 6329/06 CRIMORG 28 DROIPEN 12 ENFOPOL 26 DATAPROTECT 4 COMIX 156.
[3] doc. 5193/06 CRIMORG 3 DROIPEN 2 ENFOPOL 3 DATAPROTECT 1 COMIX 26.

DE, DK, LV, NL, PT and SI have a general scrutiny reservation on the proposal. DK, FR, IE, NL, SE, SI and UK have a parliamentary reservation. AT, ES, FI, IT and SE have a linguistic scrutiny reservation.

2. The Commission presented its proposal to the Multidisciplinary group on organised crime (MDG) - Mixed Committee on 9 November 2005, when a first discussion ensued[4]. On 12 January 2006, the MDG-Mixed Committee discussed a number of questions related to the scope of the draft Framework Decision[5].

3. At the meetings of the MDG - Mixed Committee of 8 February, 9 and 31 March, 25 April and 19 May 2006 the first two chapters were discussed in-depth. At the meetings of 20 June, 7 and 25 July 2006, Chapter III was discussed.

4. *Delegations are invited to commence the discussion of Chapters IV and V.*

---

[4] doc. 14326/05 CRIMORG 135 DROIPEN 55 ENFOPOL 151 DATAPROTECT 6 COMIX 761.
[5] doc. 5485/06 CRIMORG 11 DROIPEN 5 ENFOPOL 9 DATAPROTECT 2 COMIX 62.

ANNEX

COUNCIL FRAMEWORK DECISION

of ....

on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30, Article 31 and Article 34 (2)(b) thereof,

Having regard to the proposal from the Commission,[6]

Having regard to the opinion of the European Parliament,[7]

Whereas:

(1) The European Union has set itself the objective to maintain and develop the Union as an area of freedom, security and justice; a high level of safety shall be provided by common action among the Member States in the fields of police and judicial cooperation in criminal matters.

(2) Common action in the field of police cooperation according to Article 30(1)(b) of the Treaty on European Union and common action on judicial cooperation in criminal matters according to Article 31 (1)(a) of the Treaty on European Union imply the necessity of the processing of relevant information which should be subject to appropriate provisions on the protection of personal data.

---

6 …

7 …

(3) Legislation falling within the ambit of Title VI of the Treaty on European Union should foster police and judicial cooperation in criminal matters with regard to its efficiency as well as its legitimacy and compliance with fundamental rights, in particular the right to privacy and to protection of personal data. Common standards regarding the processing and protection of personal data processed for the purpose of preventing and combating crime can contribute to achieving both aims.

(4) The Hague Programme on strengthening freedom, security and justice in the European Union, adopted by the European Council on 4 November 2004, stressed the need for an innovative approach to the cross-border exchange of law-enforcement information under strict observation of key conditions in the area of data protection and invited the Commission to submit proposals in this regard by the end of 2005 at the latest. This was reflected in the *Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union*[8].

(5) The exchange of personal data in the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear binding rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way excluding any obstruction of this cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[9] does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

---

8 OJ C 198, 12.8.2005, p. 1.

9 OJ L 281, 23.11.1995, p. 31.

(6) A legal instrument on common standards for the protection of personal data processed for the purpose of preventing and combating crime should be consistent with the overall policy of the European Union in the area of privacy and data protection. Wherever possible, taking into account the necessity of improving the efficiency of legitimate activities of the police, customs, judicial and other competent authorities, it should therefore follow existing and proven principles and definitions, notably those laid down in Directive 95/46/EC of the European Parliament and of the Council or relating to the exchange of information by Europol, Eurojust, or processed via the Customs Information System or other comparable instruments.

(7) The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union.

(8) It is necessary to specify the objectives of data protection in the framework of police and judicial activities and to lay down rules concerning the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed legitimately and in accordance with fundamental principles relating to data quality. At the same time the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardized in any way.

(8bis) The principle of accuracy of data has to be applied in the light of the nature and the purpose of the specific processing. Especially in the course of judicial proceedings data are based on the perception of a person and in some cases those data cannot be verified at all. Thus, the principle of accuracy cannot refer to the accuracy of a statement but merely to the fact that a person has given a specific statement. Also, it has to be considered that in some cases files – and, therefore, data – will be partially verified as to their content but that those data might remain in the files, for example for documentation purposes[10].

[10] This new recital is meant to explain the concept of accuracy of Article 4(1)(d). Scrutiny reservation by SE and SI. ES thought the wording should be adapted so as to bring police work more clearly in its scope.

(9) Ensuring a high level of protection of the personal data of European citizens requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States.

(10) It is appropriate to lay down at the European level the conditions under which competent authorities of the Member States should be allowed to transmit and make available personal data to authorities and private parties in other Member States.

(11) The further processing of personal data received from or made available by the competent authority of another Member State, in particular the further transmission of or making available such data, should be subject to common rules at European level.

(12) Where personal data are transferred from a Member State of the European Union to third countries or international bodies, these data should, in principle, benefit from an adequate level of protection.

(13) This Framework Decision should define the procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body.

(14) In order to ensure the protection of personal data without jeopardising the purpose of criminal investigations, it is necessary to define the rights of the data subject.

(15) It is appropriate to establish common rules on the confidentiality and security of the processing, on liability and sanctions for unlawful use by competent authorities as well as judicial remedies available for the data subject. Furthermore, it is necessary that Member States provide for criminal sanctions for particularly serious and intentionally committed infringements of data protection provisions.

(16) The establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed in the framework of police and judicial cooperation between the Member States.

(17) Such authorities should have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings. These authorities should help to ensure transparency of processing in the Member States within whose jurisdiction they fall. However, the powers of these authorities should not interfere with specific rules set out for criminal proceedings and the independence of the judiciary.

(18) A Working Party on the protection of individuals with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences should be set up and be completely independent in the performance of its functions. It should advise the Commission and the Member States and, in particular, contribute to a uniform application of the national rules adopted pursuant to this Framework Decision.

(19) Article 47 of the Treaty on European Union provides that none of its provisions shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them. Accordingly, this Framework Decision does not affect the protection of personal data under Community law, in particular, as provided for in Directive 95/46/EC of the European Parliament and of the Council , in Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[11] and in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[12].

(20) The present Framework Decision is without prejudice to the specific data protection provisions laid down in the relevant legal instruments relating to the processing and protection of personal data by Europol, Eurojust and the Customs Information System.

[11] OJ L 8, 12.1.2001, p. 1.
[12] OJ L 201, 31.7.2001, p. 37.

(21) The provisions regarding the protection of personal data, provided for under Title IV of the Convention of 1990 implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders[13] (hereinafter referred to as the "Schengen Convention") and integrated into the framework of the European Union pursuant to the Protocol annexed to the Treaty on European Union and the Treaty establishing the European Community, should be replaced by the rules of this Framework Decision for the purposes of matters falling within the scope of the EU Treaty.

(22) It is appropriate that this Framework Decision applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision JHA/2006/ … on the establishment, operation and use of the second generation Schengen information system.

(23) This Framework Decision is without prejudice to the rules pertaining to illicit access to data as foreseen in the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[14].

(24) It is appropriate to replace Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[15].

(25) Any reference to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal data should be read as reference to this Framework Decision.

---

[13] OJ L 239, 22.9.2000, p. 19.
[14] OJ L 69, 16.3.2005, p. 67.
[15] OJ C 197, 12.7.2000, p. 3.

(26) Since the objectives of the action to be taken, namely the determination of common rules for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, cannot be sufficiently achieved by the Member States acting alone, and can therefore, by reason of the scale and effects of the action, be better achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the EC Treaty and referred to in Article 2 of the EU Treaty. In accordance with the principle of proportionality as set out in Article 5 of the EC Treaty, this Framework Decision does not go beyond what is necessary to achieve those objectives.

(27) The United Kingdom is taking part in this Framework Decision, in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8 (2) of Council Decision 2000/365/EC of 29 May 2000, concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis [16].

(28) Ireland is taking part in this Framework Decision in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 6 (2) of Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis.

(29) As regards Iceland and Norway, this Framework Decision constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1(H) of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[17].

[16] OJ L 131, 1.6.2000, p. 43.
[17] OJ L 176, 10.7.1999, p. 31.

(30) As regards Switzerland, this Framework Decision constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis which fall within the area referred to in Article 1 (H) of Council Decision 1999/437/EC of 17 May 1999 read in conjunction with Article 4 (1) of the Council Decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement[18].

(31) This Framework Decision constitutes an act building on the Schengen acquis or otherwise related to it within the meaning of Article 3(1) of the 2003 Act of Accession.

(32) This Framework Decision respects the fundamental rights and observes the principles recognized, in particular by the Charter of Fundamental Rights of the European Union. This Framework Decision seeks to ensure full respect for the rights to privacy and the protection of personal data in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union,

[18] OJ L 368, 15.12.2004, p. 26.

HAS ADOPTED THIS FRAMEWORK DECISION:

CHAPTER I
OBJECT, DEFINITIONS AND SCOPE

Article 1

Object and scope

1. This Framework Decision determines common standards to ensure the protection of individuals with regard to the processing of personal data in the framework of police and judicial co-operation in criminal matters, provided for by Title VI of the Treaty on European Union[19], while safeguarding citizens' freedom and providing them with a high level of safety.

[19] CH, CZ, DK, IE and UK thought the scope of the draft Framework Decision should be confined to transfer of data between Member States and should not cover data which are processed in a purely domestic context. SE thought the scope of the draft Framework decision should be transfer of data between Member States, but that it would also have an impact on the domestic handling of data on a general level. Scrutiny reservations by CY, CZ, DE and MT.

2. This Framework Decision shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system by a competent authority for the purpose of the prevention, investigation, detection[20] or prosecution of criminal offences[21] [22].

3. This Framework Decision shall not apply to the processing of personal data by

– the European Police Office (Europol),

– the European Judicial Cooperation Unit (Eurojust),

– the Customs Information System as set up according to the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, and any amendments made thereto[23].

---

[20] DE thought that the concepts 'investigation' and 'detection' could be deleted throughout the text of the Framework Decision. They do, however, also figure in Article 13(1)(d) of the Data Protection Directive.

[21] ES pointed out that Article 1(1) gave a broader definition of the goal of the Framework Decision than Article 3(1) (now Article 1(2) and that the language of the two provisions should be aligned. It also referred to Article 11, which allows the use of data for 'the purpose of the prevention of threats to public security or to a person'. BE pointed out that, whilst it might be acceptable to use transmitted information for these goals, these should not be the primary purposes of data protection.

[22] CH, CY, CZ, DK, ES, HU, IE, IT, NO, PT and UK think that processing of personal data in connection with national security purposes is outside the scope of the draft Framework Decision, and would like express clarification of this in the instrument. MT scrutiny reservation. The UK proposed to insert a new paragraph 3a in Article 1, which would read: "For the avoidance of doubt, this Framework Decision does not apply to national security matters". COM pointed out that, in its view, the task of the service concerned was crucial and not its denomination. The concept of 'national security matters' was inadequate and not sufficiently precise according to the Commission. In its note (doc. 5193/06 CRIMORG 3 DROIPEN 2 ENFOPOL 3 DATAPROTECT 1 COMIX 26), HU has proposed a recital to clarify this.

[23] HU, IT, and SE thought that this should be drafted in a different manner so as not to exclude these instruments from the scope of the draft Framework Decision, but simply to make proviso for their specific data protection regimes. DK and ES thought the Schengen Information System should also be excluded from the scope of the draft Framework Decision.

4. This Framework Decision does not preclude Member States to provide safeguards for the protection of personal data in the context of police and judicial cooperation in criminal matters higher than those established in this Framework Decision, but such provisions may not restrict nor prohibit the disclosure of personal data to the competent authorities of other Member States for reasons connected with the protection of personal data as provided for in this Framework Decision[24].

Article 2

Definitions[25]

For the purposes of this Framework Decision:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission[26], dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

---

[24] New text at the proposal of ES. Scrutiny reservation by AT, BE, COM, DE, IT and NL.

[25] Several delegations proposed that new indents would be added with additional definitions. DE asked for a definition of 'blocking' and 'mark' and DE proposed the following definitions, based of the Prüm Treaty. "Marking "= "the marking of stored personal data without the aim of limiting their processing in future", and "blocking" = " the marking of stored personal data with the aim of limiting their processing in future". HU and SI raised the question whether a specific definition of biometric data was needed.

[26] FR linguistic reservation on the French translation of the word transfer.

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by national law or by law adopted in accordance with Title VI of the Treaty on European Union, the controller or the specific criteria for his nomination may be designated by national law or by law under Title VI of the Treaty on European Union;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

(i) 'international bodies' shall mean bodies or organisations established by international agreements[27];

[27] Reserve from DK.

(j) 'competent authorities' shall mean police, customs, judicial and other competent authorities of the Member States that are authorized by national law to detect, prevent, investigate or prosecute offences or criminal activities[28] within the meaning of Article 29 of the Treaty on European Union.

Article 3 [29]

[28] Clarification at the suggestion of HU (see doc. 5193/06 CRIMORG 3 DROIPEN 2 ENFOPOL 3 DATAPROTECT 1 COMIX 26). This change could also accommodate the concerns raised by several States (DK, NO) whose customs authorities do not have criminal powers. CZ scrutiny reservation.

[29] As several delegations (AT, DE, FI, IT) argued in favour of a merger of Articles 1 and 3, the Presidency has inserted the text of the previous Article 3 in paragraphs 2 and 3 of Article 1.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF PROCESSING OF PERSONAL DATA

Article 4

Principles relating to data quality

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes[30];

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected[31];

(d) accurate[32] and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, for which they are further processed are erased or rectified. Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished, as far as practicable, in accordance with their degree of accuracy and reliability;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

---

[30] See new text in Article 5(3). DK and UK preferred the original COM proposal.

[31] DK, IT and SE thought the purposes should be made more explicit. DE and COM argued in favour of reintroducing the words 'and/or further processed', which appear in Article 6, (c) of the DP Directive and also in the original Commission proposal.

[32] Whilst many delegations (BE, CZ, DE, DK, IE, NL, NO, PT, SE, SI and UK) have stated that the concept of 'accuracy' is a problematic one in the context of law enforcement and judicial proceedings, most (except for DE, SE and SI) seem to be able to accept the current text in combination with recital 8bis.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Article 5

Criteria for making data processing legitimate[33]

1. Member States shall provide that personal data may be processed by the competent authorities only if provided for by law.[34] [35]

2. Member States shall provide that processing of personal data is only legitimate as far as it is necessary[36] for the prevention, investigation, detection or prosecution of criminal offences[37].

3. Member States may provide that the further processing of data is legitimate as far as it is necessary for the following purposes:

i) the prevention, investigation, detection or prosecution of criminal offences other than those for which the original processing took place[38] or

---

33 DE scrutiny reservation on paragraphs 1 and 3.

34 The last part of the sentence ("necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences") has been deleted, as it is duplicates the first indent of paragraph 2. IT thought this sentence should be more specific. IE argued that paragraph 1 in its entirety was superfluous.

35 Scrutiny reservation by DE and NO related to the absence of a reference to the situation in which a data subject gives his consent to processing. The Presidency invited the Commission to propose a text to that extent. ES, FR, GR, IT and HU were opposed to the insertion of such a reference to consent, which, according to GR, made sense only in the context of data processing for commercial purposes.

36 This text was inspired by the text of article 8(2) ECHR. However, DK and SE would prefer to use the term "proportional" instead of "necessary".

37 SK suggested adding here "or the execution of a penalty imposed for a criminal offence". Should the Working Party agree with this proposal, this addition will have to be introduced in other parts of the draft Framework Decision as well (probably in Art. 1(2)) in order to arrive at a coherent text. UK queried whether the prosecution of civil offences would be covered by the current text of Article 5(2).

38 AT suggested to add a paragraph similar to that of Article 23(1)(b) of the 2000 Mutual Assistance Convention.

ii) the protection of the rights and freedoms of a person; or

iii) the prevention of threats to public security or for other imperative reasons of overriding[39] public interest; or

iv) historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards[40].

Article 6

Processing of special categories of data[41]

In addition to the conditions laid down in Article 5, Member States shall permit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life only when this is strictly necessary. Member State shall provide for suitable additional safeguards.

Article 7

Time limits for storage of personal data [42]

1. Member States shall provide that personal data shall be stored only as long as it is necessary for the purpose for which it was collected or further processed[43].

---

39 NL thought the term 'overriding' in combination with "imperative reasons" imposed a too burdensome requirement and should therefore be deleted.

40 Several delegations (NL, UK) queried whether the current text of article 5(3) would allow for the exchange of information with administrative authorities in each and every case where that was deemed necessary. DK and PT thought the wording was too narrow and should be broadened. COM, supported by GR, pleaded in favour of a solution analogous to the one contained in article 6 of Regulation 45/2001 on data protection in the Community Institutions. ES pointed out that the Regulation was directly applicable, whereas this draft Framework Decision would need to be transposed by the Member States.

41 Scrutiny reservations by DE, DK and FR. IT thought the current text was probably too flexible.

42 Scrutiny reservation by FR, IT and NL. ES thought that the text should be changed so as to take specific account of data in judicial files.

43 NL, supported by DK, proposed that the following phrase be added: ", unless national law provides fixed and more limited periods". This idea is, however, already contained in paragraph 2. The proposed wording could moreover be construed as implying that data can be stored even if it is no longer necessary.

2. Member States shall provide for appropriate time limits for the storage of personal data or for a periodic review of the necessity of the storage and shall provide for procedural and technical measures to ensure that these are observed. Personal data shall be deleted if a review shows that their storage is no longer necessary[44].

[44] Text proposed by COM.

CHAPTER III – Specific Forms of Processing

SECTION I – TRANSMISSION OF AND MAKING AVAILABLE PERSONAL DATA TO THE COMPETENT AUTHORITIES OF OTHER MEMBER STATES

Article 8

Transmission of and making available personal data to the competent authorities of other Member States

Member States shall provide that personal data shall only be transmitted or made available to the competent authorities of other Member States in accordance with the rules of Chapter II[45].

[45] The Presidency has substituted these words for the original text ("if necessary for the purpose of the prevention, investigation, detection or prosecution of criminal offences"). The Presidency hopes this will also allay the concerns expressed by BE, DE, DK, ES, FR and SE that the transmitting authority cannot control, let alone vouch for the necessity of the transmission of these informations. The suggestion from SE of adding here "or the execution of a penalty imposed for a criminal offence", will need to be discussed in the context of other provisions (e.g. Article 5(3)(i)).

Article 9

Verification of quality of data that are transmitted or made available[46]

1. Member States shall take all reasonable steps to provide that personal data which are no longer accurate or up to date are not transmitted or made available to other Member States[47]. To that end, Member States shall provide that, as far as practicable, the quality of personal data is verified before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy[48] or reliability[49].

1bis. If personal data were transmitted without request the receiving authority shall verify without delay whether these data are necessary for the purpose for which they were transmitted.

---

[46] Several delegations (DK, DE, FR, IT, SE) thought that this provision was too detailed and should be simplified. The Presidency has attempted to do so.

[47] Text of previous paragraph 3. NL thought this paragraph was essential. UK pointed out that, in order to make it consistent with Article 4(1)(d), it should allowed for varying degrees of accuracy. DK and FR also thought the wording should be adapted. The Presidency has endeavoured to do that.

[48] DE opposed an absolute requirement to check the accuracy of law enforcement data before transmitting them. First, this requirement from the Council of Europe Recommendation is qualified in that recommendation by the words "in as far as possible". Second, it would impose a disproportionate burden on the *Bundeskriminalamt* (BKA) to require it to check the accuracy of all data it had received from *Landeskriminalamte* (LKAs) before transmitting these to other Member States' authorities. The UK queried what was the exact scope of the obligations to flow from this provision: should, for example, the accuracy of addresses contained in a law enforcement database be verified again before transmitting them? The previously mentioned requirement to check data based on opinions or personal assessments also met with scepticism (DE, NL) as to its feasibility, e.g. with regard to covertly obtained data.

[49] A recital could give further examples of this rule.

2.[50].

3.[51].

4. Member States shall provide that a competent authority that transmitted or made available personal data to a competent authority of another Member State shall inform the latter immediately if it should emerge, from a notification by the data subject or otherwise, that the data concerned should not have been transmitted or made available or that inaccurate or outdated data were transmitted or made available[52]. If the receiving authority has reasonable grounds to believe that received personal data are inaccurate or to be deleted, it shall inform without delay the competent authority that transmitted or made available the data concerned[53].

5.[54].

6. Member States shall, without prejudice to national criminal procedure[55], provide that personal data are marked on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority[56].

---

50 In view of the opinion of several Member States (DE, DK, IT and SE) that this paragraph should be deleted, the Presidency deleted it. BE also thought there was a risk that the text proposed by the Commission would impose higher obligations in a cross-border than in a purely domestic context. BE thought it was necessary but also sufficient that the receiving Member State was made aware of the quality of the data.

51 The text of this paragraph has been moved to paragraph 1.

52 DK, FR and NL could accept this paragraph. SE and UK thought care should be taken that it could not be applied retroactively, i.e. to data exchanged before the entry into force of this Framework Decision.

53 Text previously in paragraph 5. DK, FR and NL could accept this text. SE had strong doubts on this paragraph, and in particular on its compatibility with the freedom of the press. UK proposed to add at end the following wording: "or annotate the file accordingly".

54 Text integrated in paragraph 4.

55 The concept of national criminal procedure should be further clarified.

56 DK thought this paragraph did not belong in this Article, but should be placed in the chapter dealing with data subjects' rights. ES and NL had qualms with regard to general economy of this paragraph: the marking should take place only on the basis of a court decision, as is provided for in the Prüm Treaty.

7. Member States shall provide that personal data received from the authority of another Member State are deleted

– [57],

– after a time limit laid down in the law of the other Member State if the authority that transmitted or made available the data concerned has informed the receiving authority of such a time limit when the data concerned were transmitted or made available[, unless the personal data are further needed for judicial proceedings][58],

– [59].

8.[60]

9. Personal data shall not be deleted but blocked in accordance with national law if there are reasonable grounds to believe that the deletion could affect the interests of the data subject worthy of protection. Blocked data shall only be used or transmitted for the purpose they were not deleted for[61].

---

57 The Presidency deleted this indent, as the idea is already contained in paragraph 4.

58 DE scrutiny reservation , because there certain absolute time limits under DE law. AT queried why there was an exception for judicial proceedings, which did not feature in the Prüm Treaty. The question as to whether the internal time limits of the transmitting Member State should be binding on the receiving Member State, will need to be further discussed.

59 The Presidency deleted this indent, as the idea is already contained in Article 7(1).

60 See new paragraph 1bis.

61 NL scrutiny reservation. ES and NL thought the legal consequences of blocking should be better defined. NL also queried why there was a reference to national law in this paragraph, but not in paragraph 6.

Article 10

Logging and documentation[62]

1. Member States shall ensure that (...)[63] all[64] exchanges of personal data are logged or documented[64] for the purposes of verification of the admissibility of data searches and the lawfulness of the data processing, self-monitoring, ensuring proper data integrity and security[65].

2. The authority that has logged or documented such information shall communicate it without delay to the competent supervisory authority on request of the latter. The competent supervisory authority shall use this information only[66] for the control of data protection and for ensuring proper data processing as well as data integrity[67] and security and for ensuring the proper information to the data subject (....).

---

62 DE and PT scrutiny reservation. AT would have preferred that the provision list the data to be logged, as is the case in Article 39 of the Prüm Treaty.

63 The Presidency proposes to delete the words "every access to", so as to make it clear that the logging obligation applies only in cases of international o-operation and not in domestic situations. AT, BE and HU would have preferred the rules on logging to be generally applicable rules, also for domestic situations. DE, IE, SE and UK opposed this.

64 It is the Presidency's understanding that this covers both automated and non-automated exchanges, hence the terms “logged” or “documented”.

65 The UK delegation queried what would be the relation of the logging obligation to the time limits for storage under Article 7.

66 Presidency proposal in order to make it clear that this restriction applies solely to the supervisory authority that has obtained logging information.

67 DE asked that the concept 'integrity' be deleted, as it was already covered by 'security'. COM, however, stated that these were two distinct concepts.

SECTION II – FURTHER PROCESSING, IN PARTICULAR FURTHER TRANSMISSION AND TRANSFER, OF DATA RECEIVED FROM OR MADE AVAILABLE BY THE COMPETENT AUTHORITIES OF OTHER MEMBER STATES

Article 11

Further processing [and transmission][68] of personal data received from or made available by the competent authority of another Member State

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are only further processed, including their further transmission[68] or making available to other authorities of another Member State [or made available to private parties in their own Member State][69], in accordance with the rules of Articles 4, 5 and 6[70], for the purposes referred to in Article 5(3)[71].

---

[68] DE and UK queried whether it was necessary to use the concept of further transmitting, as this was already covered by the concept of processing. The Presidency is inclined to agree. CH expressed its concerns as to whether the further transmission by a receiving Member State to its own authorities would still be allowed. The Presidency deems that this is covered by the concept of further processing. As to the further transmission to private parties in another Member State, the Presidency does not think this needs to be allowed for.

[69] Various Member States (DE, FR) have questioned the need to regulate this. Pending further explanations by the Commission, the Presidency has placed this in square brackets.

[70] The new proposed wording of Article 11 raises the question as to whether Article 8 should be kept as a separate provision.

[71] At the suggestion of several delegations, the Presidency has replaced the substantial rules previously contained in this paragraph by a general reference to Article 5(3). Some delegations, however, thought the reference to Article 5(3) was too broad and would prefer to limit the purposes of processing to those for which the data was transmitted (specialty principle): BE, CH and FR. Scrutiny reservations by CH, FR and GR. The Presidency, however, deems it consistent to allow for further processing in the receiving Member State of the already transmitted personal data in conformity with the general rules on the lawfulness of processing of personal data and for the same purposes as in the transmitting Member State.

2. Processing for any other purposes shall take place only with the prior consent of the competent authority that transmitted or made available the personal data[72].

3. [Paragraph 1 shall not apply if specific legislation under Title VI of the Treaty on European Union explicitly stipulates that personal data received from or made available by the competent authority of another Member State shall only be further processed or further transmitted or only be further transmitted under more specific conditions for the purposes they were transmitted or made available for.][73]

Article 12

Transmission to other competent authorities

(....)[74]

Article 13

Transmission to authorities other than competent authorities

(....)[75]

Article 14

Transmission to private parties

(....)[76]

---

[72] The Presidency suggests to confine the additional requirement of prior consent to processing for any other purposes than those referred to in Article 5(3). DE correctly pointed out it does not make sense to combine this requirement with the substantial rules. ES also indicated that this would amount to a more stringent requirement than that of Article 23 of the 2000 Mutual Assistance Convention, where the prior consent is only required to allow the processing for other purposes. The UK delegation, however, asked that consent of the data subject be retained as a valid, alternative, basis for further processing

[73] Various delegations (BE, DE, DK, NL and UK) thought there was no need for such paragraph. The Presidency proposes to deal with the question of the relationship of this Framework Decision to other, more specific data protection provisions, in a more general way at a later stage.

[74] Article 11 has been amended so as to cover the situation previously described in this article.

[75] Article 11 has been amended so as to cover the situation previously described in this article.

[76] Article 11 has been amended so as to cover the situation previously described in this article.

Article 15

Transfer to competent authorities in third countries or to international bodies[77]

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

   (a) The transfer is provided for by law clearly obliging or authorising it.

   (b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

   (c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer[78].

---

[77] The Commission proposal to confine the scope this provision to data received from other Member States was supported by CZ, CH, ES, NL and PL. A number of Member States thought that the Framework Decision should not deal with the transfer of data to third countries: DE, DK, IE, NO, SE and UK. Four Member States thought this provision should be extended to all data: BE, FI, HU, PT. DK, ES, NO and UK thought there was no legal basis for this. Some Member States referred to Article 2 of the Additional Protocol to the 1981 Data Protection Convention. This Protocol has so far been ratified by 9 Member States.

[78] IE, NO and SE deem that this condition suffices and that there is no need for an adequacy finding as provided for in Article 15. BE thought it was the only reasonable option, should the Council decide to confine the scope of Article 15 to data received from other Member States, as any adequacy requirement could in that case be circumvented by asking the data directly to the originating Member State.

(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred[79].

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. [Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary[80] to prevent any transfer of personal data to the third country or international body in question.]

5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

---

[79] CZ, CH, FI, GR and PT supported the requirement of an adequacy finding. The Commission pointed out that that is proposal, containing both the requirement of prior consent and of an adequacy finding, sought to reconcile data protection and operational concerns. DE, DK, ES, IE, NO, SE and UK were opposed to the requirement of an adequacy finding. It was thought, *inter alia*, that this procedure was too complex and did not work adequately in the context of the Data Protection Directive.

[80] PL queried what should by understood by ' measures necessary '.

6. By way of derogation from paragraphs 1(d) and (2) , personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order:

(a) to safeguard the essential interests of a Member State; or

(b) for the prevention of imminent serious danger threatening public security or a specific person or persons; or

(c) the data subject has given his consent to the proposed transfer; or

(d) the transfer is necessary in order to safeguard the vital interests of the data subject[81].

[Article 16

Committee[82]

1. Where reference is made to this Article, the Commission shall be assisted by a Committee composed of the representatives of the Member States and chaired by the representative of the Commission[83].

---

81 The Presidency has followed up on the suggestion of various delegations (BE, CH and NL) to enlarge the exceptional cases in which it would be possible to transfer data notwithstanding the fact that there is no adequate data protection level in the third country concerned. The exceptions (c) and (d) figure also in Article 26(1) of the 1995 Data Protection Directive. As has been made clear by various delegations, there is a need to exchange data with third countries, in particular in the context of terrorism fighting, even in the absence adequate data protection level in the third country concerned.

82 The comitology procedure proposed in this provision was supported by only two Member States (FI and HU). CZ, DE, DK, ES, FR, IT, NO, and SE were opposed to it. AT and PT have a scrutiny reservation.

83 CH and NO have queried what the position of the so-called COMIX states would be in this Committee.

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the Official Journal of the European Union.

3. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the chairperson may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty establishing the European Community, in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairperson shall not vote.

4. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall, without delay, submit to the Council a proposal relating to the measures to be taken and shall inform the European Parliament thereof.

5. The Council may act by qualified majority on the proposal, within two months from the date of referral to the Council.

   If within that period, the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, resubmit its proposal or present a legislative proposal. If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

Article 17

Exceptions from Article 15[84]

Article 15 shall not apply if specific legislation under Title VI of the Treaty on European Union explicitly stipulates that personal data received from or made available by the competent authority of another Member State shall not be further transmitted or only be further transmitted under more specific conditions[85].

Article 18

Information on request of the competent authority

The receiving Member State can, in specific cases, be requested by the competent authority from or by whom personal data were received or made available to give information about their use and further processing (...)[86].

---

84 CZ and DE scrutiny reservation.

85 AT, ES and FI could accept the current text, but thought its scope could not be extended to more general or lenient provisions. IE, PT and UK thought there was no need for this *lex specialis* principle, even though PT could accept is a provisional solution. The Presidency proposes to deal with the question of the relationship of this Framework Decision to other, more specific data protection provisions, in a more general way at a later stage.

86 As suggested by BE, the Presidency has aligned the text with that of Article 9(4) of the draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

Article 19

Right of information in cases of collection of data from the data subject with his knowledge

1. Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with his knowledge with at least the following information free of cost, except where he already has it:

   (a) the identity of the controller and of his representative, if any;

   (b) the purposes of the processing for which the data are intended;

   (c) any further information such as

   – the legal basis of the processing,

   – the recipients or categories of recipients of the data,

   – whether replies to questions or other forms of cooperation are obligatory or voluntary, as well as the possible consequences of failure to reply or to cooperate,

   – the existence of the right of access to and the right to rectify the data concerning him or her

   in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

2. The provision of the information laid down in paragraph 1 shall be refused or restricted only if necessary

   (a) to enable the controller to fulfil its lawful duties properly,

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

3. If the information referred to in paragraph 1 is refused or restricted, the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure.

4. The reasons for a refusal or restriction according to paragraph 2 shall not be given if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure. If the data subject lodges an appeal to the supervisory authority, the latter shall examine the appeal. The supervisory authority shall, when investigating the appeal, only inform him of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

Article 20

Right of information where the data have not been obtained from the data subject or have been obtained from him without his knowledge

1. Where the data have not been obtained from the data subject or have been obtained from him without his knowledge or without his awareness that data are being collected concerning him, Member States shall provide that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, within a reasonable time after the data are first disclosed, provide the data subject with at least the following information free of cost, except where he already has it or the provision of the information proves impossible or would involve a disproportionate effort:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

– the legal basis of the processing,

– the categories of data concerned,

– the recipients or categories of recipients,

– the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. The information laid down in paragraph 1 shall not be provided if necessary

(a) to enable the controller to fulfil its lawful duties properly,

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

Article 21

Right of access, rectification, erasure or blocking

1. Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint, at reasonable intervals and without excessive delay or expense:

– confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, the legal basis of the processing and the recipients or categories of recipients to whom the data have been disclosed,

– communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;

(b) as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Framework Decision, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

2. Any act the data subject is entitled to according to paragraph 1 shall be refused if necessary

(a) to enable the controller to fulfil its lawful duties properly,

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

3. A refusal or restriction of the rights referred to in paragraph 1 shall be set out in writing. If the right referred to in paragraph 1 is refused or restricted, the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure.

4. The reasons for a refusal according to paragraph 2 shall not be given to the data subject if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure. If the data subject lodges an appeal to the supervisory authority, the latter shall examine the appeal. The supervisory authority shall, when investigating the appeal, only inform him of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

Article 22

Information to third parties following rectification, blocking or erasure

Member States shall provide that appropriate technical measures are taken to ensure that, in cases where the controller rectifies, blocks or erases personal data following a request, a list of the suppliers and addressees of these data is automatically produced. The controller shall ensure that those included in the list are informed of the changes performed on the personal data.

CHAPTER V

Confidentiality and security of processing

Article 23

Confidentiality

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law. All persons called upon to work with or within a competent authority of a Member State shall be bound by strict confidentiality rules.

Article 24

Security

1. Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected.

   Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Measures shall be deemed necessary where the effort they involve is not disproportionate to the objective they are designed to achieve in terms of protection.

2. In respect of automated data processing each Member State shall implement measures designed to:

(a) deny unauthorized persons access to data processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorized reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorized input of data and the unauthorized inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data processing systems by unauthorized persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be immediately restored (recovery);

(j) ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

4. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

– the processor shall act only on instructions from the controller,

– the obligations set out in paragraphs 1 and 2, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

5. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 25

Register

1. Member States shall provide that every controller keeps a register of any processing operation or sets of such an operation intended to serve a single purpose or several related purposes. The information to be contained in the register shall include

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the legal basis of the processing operation for which the data are intended;

(e) the recipients or categories of recipient to whom the data might be disclosed;

(f) proposed transfers of data to third countries;

(g) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 24 to ensure security of processing.

2. Member States shall specify the conditions and procedures under which information referred to in paragraph 1 must be notified to the supervisory authority.

Article 26

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

CHAPTER VI
JUDICIAL REMEDIES AND LIABILITY

Article 27

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 30, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law pursuant to this Framework Decision to the processing in question.

Article 28

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

2. However, a competent authority that received personal data from the competent authority of another Member State is liable vis-à-vis the injured party for damages caused because of the use of inaccurate or outdated data. It can not disclaim its liability on the ground that it received inaccurate or outdated data from another authority. If damages are awarded against the receiving authority because of its use of inaccurate data transmitted or made available by the competent authority of another Member State, the latter shall refund in full to the receiving authority the amount paid in damages.

Article 29

Sanctions

1. The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision and shall in particular lay down effective, proportionate and dissuasive sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Framework Decision.

2. Member States shall provide for effective, proportionate and dissuasive criminal sanctions for intentionally committed offences implying serious infringements of provisions adopted pursuant to this Framework Decision, notably provisions aimed at ensuring confidentiality and security of processing.

CHAPTER VII

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 30

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Framework Decision. These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

3. Each authority shall in particular be endowed with:

   – investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

   – effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 26, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

– the power to engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

7. The supervisory authorities shall cooperate with one another as well as with the supervisory bodies set up under Title VI of the Treaty on European Union and the European Data Protection Supervisor to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

8. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

9. The powers of the supervisory authority shall not affect the independence of the judiciary and the decision taken by this authority shall be without prejudice to the execution of the legitimate tasks of the judiciary in criminal proceedings.

Article 31

Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the prevention, investigation, detection and prosecution of criminal offences

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the prevention, investigation, detection and prosecution of criminal offences, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State, of a representative of the European Data Protection Supervisor, and of a representative of the Commission.

   Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative.

   The chairpersons of the joint supervisory bodies set up under Title VI of the Treaty on European Union shall be entitled to participate or to be represented in meetings of the Working Party. The supervisory authority or authorities designated by Iceland, Norway and Switzerland shall be entitled to be represented in meetings of the Working Party insofar as issues related to the Schengen Acquis are concerned.

3. The Working Party shall take its decisions by a simple majority of the representatives of the supervisory authorities of the Member States.

4. The Working Party shall elect its chairperson. The chairperson's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairperson, either on his own initiative or at the request of a representative of the supervisory authorities, the Commission, the European Data Protection Supervisor or the chairpersons of the joint supervisory bodies.

Article 32

Tasks

1. The Working Party shall,

   (a) examine any question covering the application of the national measures adopted under this Framework Decision in order to contribute to the uniform application of such measures,

   (b) give an opinion on the level of protection in the Member States and in third countries and international bodies, in particular in order to guarantee that personal data are transferred in compliance with Article 15 of this Framework Decision to third countries or international bodies that ensure an adequate level of data protection,

   (c) advise the Commission and the Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and on any other proposed measures affecting such rights and freedoms.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the European Union are arising between the laws and practices of Member States it shall inform the Council and the Commission.

3. The Working Party may, on its own initiative or on the initiative of the Commission or the Council, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the European Union for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

4. The Working Party's opinions and recommendations shall be forwarded to the Council, to the Commission and to the European Parliament and to the committee referred to in Article 16.

5. The Commission shall, based on information provided by the Member States, inform the Working Party of the action taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public. Member States shall inform the Working Party of any action taken by them pursuant to Paragraph 1.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences in the European Union and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VIII

Final provisions

Article 33

Amendment of the Schengen Convention

For the purposes of matters falling within the scope of the EU Treaty, this Framework Decision replaces Articles 126 to 130 of the Schengen Convention.

Article 34

Relation to other instruments concerning the processing and protection of personal data

1. This Framework Decision replaces Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union..

2. Any reference to the Convention No 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data shall be construed as a reference to this Framework Decision.

Article 35

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision on 31 December 2006.

2. By the same date Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into national law the obligations imposed on them under this Framework Decision, as well as information on the designation of the supervisory authority or authorities referred to in Article 29. On the basis of this information and a written report from the Commission, the Council shall before 31 December 2007 assess the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

Article 36

Entry into force

This Framework Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Done at Brussels,

For the Council
The President